PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-122238
(43)Date of publication of application : 30.04.1999

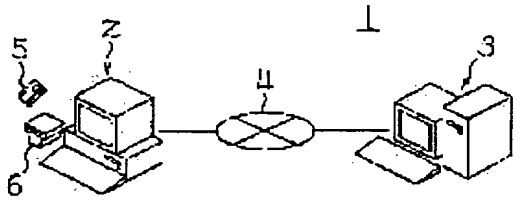
(51)Int.Cl. H04L 9/08
G06K 17/00
G09C 1/00
H04L 9/14
H04L 9/32

(21)Application number : 09-284785
(22)Date of filing : 17.10.1997

(71)Applicant : RICOH CO LTD
(72)Inventor : KANAI YOICHI

(54) NETWORK SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a network system capable of updating an authentication key independently of whether the communication algorithm is a symmetry key cipher system or an asymmetry key cipher system.
SOLUTION: After mutual authentication conducted by using an (m-1)th internal authentication key and an (n-1)th external authentication key is established, a server 3 sends random numbers Rk1, Rk2 to a client 2, the random numbers Rk1, Rk2 are encrypted by using the (m-1)th internal authentication key and the (n-1)th external authentication key used for the mutual authentication to generate newly the m-th internal authentication key and the n-th external authentication key and they are stored in a nonvolatile memory.



LEGAL STATUS

[Date of request for examination] 17.02.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－122238

(43)公開日　平成11年(1999)４月30日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｄ
Ｇ０６Ｋ	17/00		Ｇ０６Ｋ	17/00	Ｔ
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｅ
Ｈ０４Ｌ	9/14		Ｈ０４Ｌ	9/00	６０１Ｅ
	9/32				６４１

審査請求　未請求　請求項の数11　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平9－284785

(22)出願日　平成９年(1997)10月17日

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号

(72)発明者　金井　洋一
東京都大田区中馬込１丁目３番６号　株式会社リコー内

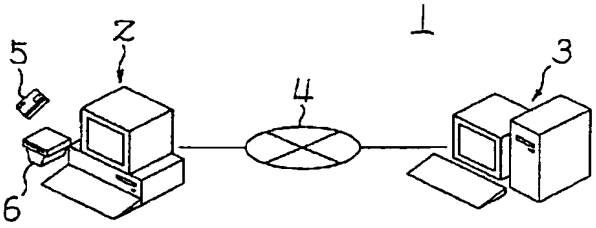
(74)代理人　弁理士　柏木　明　（外１名）

(54)【発明の名称】　ネットワークシステム

(57)【要約】

【課題】　通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、認証鍵を更新することができるネットワークシステムを提供する。

【解決手段】　（ｍ－１）番の内部認証鍵と、（ｎ－１）番の外部認証鍵を用いて行なう相互認証が成立した後に、サーバ３から乱数Ｒｋ１、Ｒｋ２をクライアント２に送信し、前記相互認証に用いた（ｍ－１）番の内部認証鍵と、（ｎ－１）番の外部認証鍵を用いて乱数Ｒｋ１、Ｒｋ２を暗号化して、ｍ番の内部認証鍵とｎ番の外部認証鍵を新たに生成して、不揮発性メモリに記憶する。



【特許請求の範囲】

【請求項１】　通信回線を介して接続されているクライアントとサーバとの間の相互認証に使用する認証鍵を格納している記憶媒体をユーザが所持し、この記憶媒体と前記クライアントを接続して、前記認証鍵を用いた前記相互認証を行なった後、前記認証鍵に基づいてセッション鍵を生成して暗号化通信を行なうネットワークシステムであって、

前記認証鍵は前記記憶媒体に複数個記憶して、定期または不定期に更新して用い、

この更新を前記複数の認証鍵のうちいずれかのものに対して行なうには、少なくとも当該認証鍵以外の前記認証鍵を用いて行なう前記相互認証が成立した後に、前記サーバから乱数を前記クライアントに送信し、前記相互認証に用いた前記認証鍵を用いて前記乱数から更新にかかる前記認証鍵を新たに生成して前記記憶媒体に記憶することにより行なうものであることを特徴とするネットワークシステム。

【請求項２】　記憶媒体は、クライアントがサーバを認証するための認証鍵である外部認証鍵と、前記サーバが前記クライアントを認証するための認証鍵である内部認証鍵とをいずれも識別番号を付して複数個ずつ記憶していて、前記内部認証鍵および前記外部認証鍵を用いて相互認証を行なうものであることを特徴とする請求項１に記載のネットワークシステム。

【請求項３】　複数の内部認証鍵のうち識別番号がｍ番のものを更新するには、外部認証鍵と少なくともこのｍ番の内部認証鍵以外の内部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記ｍ番の内部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とする請求項２に記載のネットワークシステム。

【請求項４】　複数の外部認証鍵のうち識別番号がｎ番のものを更新するには、内部認証鍵と少なくともこのｎ番の外部認証鍵以外の外部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記ｎ番の外部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とする請求項１または２に記載のネットワークシステム。

【請求項５】　複数の内部認証鍵のうち識別番号がｍ番のものおよび複数の外部認証鍵のうち識別番号がｎ番目のものを一度に更新するには、少なくとも前記ｍ番の内部認証鍵以外の内部認証鍵と少なくとも前記ｎ番の外部認証鍵以外の外部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記ｍ番の内部認証鍵と前記ｎ番の外部認証鍵とを新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とする請求項２、３、４のいずれかに記載のネットワークシステム。

【請求項６】　複数の内部認証鍵を一度に更新するには、外部認証鍵と識別番号がｍ番より小さい内部認証鍵とを用いて相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記識別番号がｍ番以上の各内部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とする請求項２、３、４、５のいずれかに記載のネットワークシステム。

【請求項７】　複数の外部認証鍵を一度に更新するには、内部認証鍵と識別番号がｎ番より小さい外部認証鍵とを用いて相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記識別番号がｎ番以上の各外部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とする請求項２、３、４、５、６のいずれかに記載のネットワークシステム。

【請求項８】　複数の内部認証鍵と複数の外部認証鍵とを一度に更新するには、識別番号がｍ番より小さい内部認証鍵と識別番号がｎ番より小さい外部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から識別番号がｍ番以上の内部認証鍵と識別番号がｎ番移動の外部認証鍵とを新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とする請求項２、３、４、５、６、７のいずれかに記載のネットワークシステム。

【請求項９】　更新の際の内部認証鍵の総数をＭ、外部認証鍵の総数をＮとしたときに、下式で示されるｍ番目の内部認証鍵とｎ番目の外部認証鍵の更新は、識別番号が少なくともｎ番より小さい番号の外部認証鍵を用いてクライアントがサーバを認証したことを条件に行なうものであることを特徴とする請求項２、３、４、５、６、７、８のいずれかに記載のネットワークシステム。

Ｍ－ｍ＝Ｎ－ｎ

【請求項１０】　記憶媒体は、

更新に先立って行なわれた相互認証に使用した認証鍵を用いサーバがクライアントに送信した乱数から新たな認証鍵の生成を行なって、この生成後の新たな認証鍵を記憶媒体内部の不揮発性メモリにのみ記憶するものであることを特徴とする請求項１、２、３、４、５、６、７、８、９のいずれかに記載のネットワークシステム。

【請求項１１】　記憶媒体としてＩＣカードを用いることを特徴とする請求項１、２、３、４、５、６、７、８、９、１０のいずれかに記載のネットワークシステ

ム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明はネットワークシステムに関し、特に、クライアントとサーバとの間の相互認証に関する。

【０００２】

【従来の技術】特開平６－１５００８２号公報には、ＩＣカードを所持したユーザが、このＩＣカードに記録されている秘密情報を用い、通信回線を介しクライアントからサーバに対して認証を要求する技術に関するものであり、非対称鍵暗号方式の暗号アルゴリズムを用いてＩＣカード内の秘密情報を変更する技術が開示されている。

【０００３】

【発明が解決しようとする課題】しかしながら、前記従来技術は、秘密鍵と公開鍵を用いる非対称鍵暗号方式の暗号アルゴリズムをＩＣカードに搭載してＩＣカード内の秘密情報を変更する技術が開示されているにとどまり、対称鍵暗号方式を用いる場合にＩＣカード内の秘密情報を変更するための技術はなんら開示されていない。

【０００４】この発明の目的は、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、認証鍵を更新することができるネットワークシステムを提供することにある。

【０００５】この発明の別の目的は、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、内部認証鍵や外部認証鍵を更新することができるネットワークシステムを提供することにある。

【０００６】この発明の別の目的は、少ない鍵更新処理により安全に、内部認証鍵や外部認証鍵を更新することができるネットワークシステムを提供することにある。

【０００７】この発明の別の目的は、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、使用が稀である認証鍵により使用が頻繁な内部認証鍵や外部認証鍵を安全に更新することができるネットワークシステムを提供することにある。

【０００８】この発明の別の目的は、更新後の新たな認証鍵を記憶媒体外に漏らすことなく認証鍵を安全に更新することができるネットワークシステムを提供することにある。

【０００９】この発明の別の目的は、ネットワークシステムを低コストで構築することにある。

【００１０】

【課題を解決するための手段】請求項１に記載の発明は、通信回線を介して接続されているクライアントとサーバとの間の相互認証に使用する認証鍵を格納している記憶媒体をユーザが所持し、この記憶媒体と前記クライアントを接続して、前記認証鍵を用いた前記相互認証を行なった後、前記認証鍵に基づいてセッション鍵を生成して暗号化通信を行なうネットワークシステムであって、前記認証鍵は前記記憶媒体に複数個記憶して、定期または不定期に更新して用い、この更新を前記複数の認証鍵のうちいずれかのものに対して行なうには、少なくとも当該認証鍵以外の前記認証鍵を用いて行なう前記相互認証が成立した後に、前記サーバから乱数を前記クライアントに送信し、前記相互認証に用いた前記認証鍵を用いて前記乱数から更新にかかる前記認証鍵を新たに生成して前記記憶媒体に記憶することにより行なうものであることを特徴とするものである。

【００１１】従って、相互認証が成立した後に、サーバから乱数をクライアントに送信し、相互認証に用いた認証鍵を用いて乱数から更新にかかる認証鍵を新たに暗号化や復号化などで生成することができるので、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、認証鍵を更新することができる。

【００１２】請求項２に記載の発明は、記憶媒体は、クライアントがサーバを認証するための認証鍵である外部認証鍵と、前記サーバが前記クライアントを認証するための認証鍵である内部認証鍵とをいずれも識別番号を付して複数個ずつ記憶していて、前記内部認証鍵および前記外部認証鍵を用いて相互認証を行なうものであることを特徴とするものである。

【００１３】従って、相互認証が成立した後に、サーバから乱数をクライアントに送信し、相互認証に用いた内部認証鍵を用いて乱数から更新にかかる内部認証鍵、外部認証鍵を新たに生成することができるので、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、内部認証鍵、外部認証鍵を更新することができる。

【００１４】請求項３に記載の発明は、複数の内部認証鍵のうち識別番号がm番のものを更新するには、外部認証鍵と少なくともこのm番の内部認証鍵以外の内部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記m番の内部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものである。

【００１５】従って、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、識別番号がm番の内部認証鍵を更新することができる。

【００１６】請求項４に記載の発明は、複数の外部認証鍵のうち識別番号がｎ番のものを更新するには、内部認証鍵と少なくともこのｎ番の外部認証鍵以外の外部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記ｎ番の外部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするもので

ある。

【００１７】従って、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに識別番号がｎ番の外部認証鍵を更新することができる。

【００１８】請求項５に記載の発明は、複数の内部認証鍵のうち識別番号がｍ番のものおよび複数の外部認証鍵のうち識別番号がｎ番目のものを一度に更新するには、少なくとも前記ｍ番の内部認証鍵以外の内部認証鍵と少なくとも前記ｎ番の外部認証鍵以外の外部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記ｍ番の内部認証鍵と前記ｎ番の外部認証鍵とを新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものである。

【００１９】従って、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、少ない鍵更新処理により安全に、識別番号がｍ番の内部認証鍵と識別番号がｎ番の外部認証鍵を一度に更新することができる。

【００２０】請求項６に記載の発明は、複数の内部認証鍵を一度に更新するには、外部認証鍵と識別番号がｍ番より小さい内部認証鍵とを用いて相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記識別番号がｍ番以上の各内部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものである。

【００２１】従って、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、少ない鍵更新処理により安全に、複数の内部認証鍵を一度に更新することができる。

【００２２】請求項７に記載の発明は、複数の外部認証鍵を一度に更新するには、内部認証鍵と識別番号がｎ番より小さい外部認証鍵とを用いて相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記識別番号がｎ番以上の各外部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものである。

【００２３】従って、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、少ない鍵更新処理により安全に、複数の外部認証鍵を一度に更新することができる。

【００２４】請求項８に記載の発明は、複数の内部認証鍵と複数の外部認証鍵とを一度に更新するには、識別番号がｍ番より小さい内部認証鍵と識別番号がｎ番より小さい外部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から識別番号がｍ番以上の内部認証鍵と識別番号がｎ番移動の外部認証鍵とを新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものである。

【００２５】従って、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、少ない鍵更新処理により安全に、複数の内部認証鍵と複数の外部認証鍵とを一度に更新することができる。

【００２６】請求項９に記載の発明は、更新の際の内部認証鍵の総数をＭ、外部認証鍵の総数をＮとしたときに、下式で示されるｍ番目の内部認証鍵とｎ番目の外部認証鍵の更新は、識別番号が少なくともｎ番より小さい番号の外部認証鍵を用いてクライアントがサーバを認証したことを条件に行なうものであることを特徴とするものである。

【００２７】Ｍ－ｍ＝Ｎ－ｎ

従って、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、使用が稀である認証鍵により使用が頻繁な認証鍵ｍ番目の内部認証鍵とｎ番目の外部認証鍵とを安全に更新することができる。

【００２８】請求項１０に記載の発明は、記憶媒体は、更新に先立って行なわれた相互認証に使用した認証鍵を用いサーバがクライアントに送信した乱数から新たな認証鍵の生成を行なって、この生成後の新たな認証鍵を記憶媒体内部の不揮発性メモリにのみ記憶するものであることを特徴とするものである。

【００２９】従って、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、更新後の新たな認証鍵を記憶媒体外に漏らすことなく認証鍵を安全に更新することができる。

【００３０】請求項１１に記載の発明は、記憶媒体としてＩＣカードを用いることを特徴とするものである。

【００３１】従って、一般に普及し始めているＩＣカードを記憶媒体として用い、ネットワークシステムを低コストで構築することができる。

【００３２】

【発明の実施の形態】

〔発明の第１の実施の形態〕図１は、この発明のネットワークシステムを実現した、この発明の第１の実施の形態である対称鍵暗号系を使用したネットワークシステム１の概略システム構成のブロック図である。

【００３３】ネットワークシステム１は、クライアント２と、このクライアントを管理するクライアント管理データベース（図示せず）を備えたサーバ３とを通信回線４で接続したクライアント／サーバシステムである。

【００３４】クライアント２には、ＩＣカード５に対してデータの書き込み、読み取りを行なうＩＣカードリーダライタ６が接続されている。

【００３５】サーバ３は、ＩＣカード５の配布元や、後述する秘密鍵の発行センタをも兼ねている。すなわち、

サーバ３は、各ユーザに対応して、ユーザ用に秘密鍵をm組生成し、また、サーバ３用に秘密鍵をｎ組生成する（このサーバ３用に秘密鍵は、各ユーザごとに生成せずに、全ユーザ共通としてもよい）。そして、サーバ３のクライアント管理データベースには、サーバ３が生成したすべての秘密鍵を記憶する。

【００３６】ＩＣカード５は、この発明の記憶媒体を実現するもので、例えば、図２に示すように、マイクロプロセッサ１１と、このマイクロプロセッサ１１と接続され、データの書替えが可能な不揮発性メモリ１２（ＥＥＰＲＯＭ〔この発明の記憶手段を実現するものである〕）と、マイクロプロセッサ１１とＩＣカードリーダライタ６との間のデータの授受を行なうインターフェイスである入出力装置１３などが搭載されていて、国際規格（ＩＳ）で規定されている、“Internal Authentication コマンド”、“External Authentication コマンド”、“Get Challenge コマンド”をサポートしているものである。

【００３７】マイクロプロセッサ１１のＲＯＭには、クライアント２とサーバ３との間の相互認証を行なう暗号アルゴリズムが記憶されている。この暗号アルゴリズムはサーバ３（のＲＯＭ）にも格納されている。このマイクロプロセッサ１１およびサーバ３のＲＯＭに記憶されている相互認証のための暗号アルゴリズムは非対称鍵暗号方式のものである。

【００３８】図３は、不揮発性メモリ１２内の認証鍵のファイルフォーマットの一例を示すブロック図である。このファイルフォーマットは、主ファイルＭＦの下位に専用ファイルＤＦを有し（図３の例では、専用ファイルＤＦ１、ＤＦ２、ＤＦ３を有している）、この専用ファイルＤＦの下位に基礎ファイルＩＥＦを有する（図３の例では、専用ファイルＤＦ１の下位に基礎ファイルＩＥＦ１、ＩＥＦ２、ＩＥＦ３、ＩＥＦ４、ＩＥＦ５、ＩＥＦ６、ＩＥＦ７を有している）階層構造をなしている。基礎ファイルＩＥＦには、前記したようにサーバ３でユーザ用に生成したm組の秘密鍵を内部認証鍵として記憶し、サーバ３用に生成したｎ組の秘密鍵を外部認証鍵として記憶する。

【００３９】また、サーバ３のクライアント管理データベースにもユーザ用に生成した秘密鍵m組を外部認証鍵として記憶し、サーバ３用に生成した秘密鍵を内部認証鍵として記憶している。すなわち、内部認証鍵は、クライアント２がサーバ３を認証するための認証鍵であり、外部認証鍵は、サーバ３がクライアント２を認証するための認証鍵である。

【００４０】内部認証鍵および外部認証鍵は、各々順番号の識別番号が付されている。以下では、ＩＣカード５に記憶されているm番目の内部認証鍵をｋａｉ［m］のように表示し、ＩＣカード５に記憶されているｎ番目の外部認証鍵をｋａｅ［n］のように表示する。また、サーバ３で管理しているｎ番目の内部認証鍵をｋｓｉ［n］と表示し、サーバ３で管理しているm番目の外部認証鍵をｋｓｅ［m］と表示する。図３の例では、基礎ファイルＩＥＦ１、ＩＥＦ２、ＩＥＦ３、ＩＥＦ４、ＩＥＦ５、ＩＥＦ６、ＩＥＦ７の各々に、３つの内部認証鍵と４つの外部認証鍵、すなわち、ｋａｉ［１］、ｋａｉ［２］、ｋａｉ［３］、ｋａｅ［１］、ｋａｅ［２］、ｋａｅ［３］、ｋａｅ［４］が格納されている。

【００４１】ＩＣカード５は、外部認証鍵、内部認証鍵を予め記憶した状態でネットワークシステム１のユーザに配布するものとする。ユーザは、このＩＣカード５を所持し、ネットワークシステム１を利用する際には、クライアント２のＩＣカードリーダライタ６にＩＣカード５を装填してクライアント２を操作する。

【００４２】以上のようなシステム構成で、クライアント２からサーバ３に接続要求がされると、次のようにしてクライアント２とサーバ３との間の相互認証が行なわれる。図４は、この相互認証の手順を示す概念図である。なお、以下の説明で、Ｅ（Ｋ，Ｒ）は、ＲをＫで暗号化することを示し、Ｄ（Ｋ，Ｒ）は、ＲをＫで復号化することを示している。

【００４３】相互認証にはＩＣカード５に記憶されているm個の内部認証鍵、ｎ個の外部認証鍵のうち一番番号の大きい、ｋａｉ［m］、ｋａｅ［n］を用いる。まず、クライアント２から接続要求を受け取ったサーバ３は、乱数Ｒｓをクライアント２に送信する。クライアント２は、ＩＣカード５に乱数Ｒｓを送信し、ＩＣカード５のマイクロプロセッサ１１では、Ｅ（Ｋａｉ［m］，Ｒｓ）の処理、すなわち、不揮発性メモリ１２に記憶されている識別番号がm番の内部認証鍵を用いて乱数Ｒｓを暗号化することで、内部認証コードＣａｉに変換する。そして、この“内部認証コードＣａｉ＝Ｅ（Ｋａｉ［m］，Ｒｓ）”をクライアント２からサーバ３に送信する。

【００４４】すると、サーバ３では、“Ｄ（Ｋｓｅ〔m〕、Ｃａｉ）”の処理、すなわち、ＩＣカード５用の外部認証鍵のうち識別番号がm番のものをクライアント管理データベースから呼出し、この外部認証鍵を用いて、“Ｃａｉ＝Ｅ（Ｋａｉ〔m〕，Ｒｓ）”の復号化を行ない、そして、この復号化したＣａｉと乱数Ｒｓとが一致するか否かを判断する。そして、一致するときは所定のＯＫ信号を、一致しないときは所定のＮＧ信号を、クライアント２に送信する。

【００４５】このＯＫ信号を受けたときは、クライアント２はＩＣカード５に乱数を要求する。ＩＣカード５は、この信号を受けて乱数Ｒａをクライアント２に出力し、クライアント２は、この乱数Ｒａをサーバ３に送信する。サーバ３では、Ｅ（Ｋｓｉ［n］，Ｒａ）の処理を行なう。すなわち、ＩＣカード５用で識別番号がｎ番

の内部認証鍵を用いて乱数Ｒａを暗号化することにより、サーバ３の内部認証コード、すなわち、クライアント２にとっての外部認証コード“Ｃｓｉ＝Ｅ（Ｋｓｉ［ｎ］，Ｒａ）”に変換し、クライアント２に送信する。クライアント２は、この外部認証コードＣｓｉをＩＣカード５に送信し、ＩＣカード５では、“Ｄ（Ｋａｅ〔ｎ〕，Ｃｓｉ）”の処理、すなわち、不揮発性メモリ１２に記憶されているｎ番の外部認証鍵で“Ｃｓｉ＝Ｅ（Ｋｓｉ〔ｎ〕，Ｒａ）”を復号化し、復号化後の“Ｄ（Ｋａｅ〔ｎ〕，Ｃｓｉ）”が乱数Ｒａに一致するか否かを判断する。一致するときは所定のＯＫ信号を、一致しないときは所定のＮＧ信号をクライアント２に送信し、クライアント２はサーバ３にＯＫ信号、またはＮＧ信号を送信する。

【００４６】ＩＣカード５が、サーバ３から配布された正当なＩＣカードであるときは、サーバ３が管理している外部認証鍵Ｋｓｅと、ＩＣカード５に記憶されている内部認証鍵Ｋａｉとは対応し、また、ＩＣカード５に記憶されている外部認証鍵Ｋａｅと、サーバ３が管理している内部認証鍵Ｋｓｉとは対応するので、相互認証が成立する。

【００４７】次に、この相互認証の成立後に行う暗号化データ通信の手順について説明する。図５は、認証鍵を利用してセッション鍵を生成する手順を示す概念図である。セッション鍵は、クライアント２／サーバ３間で共有して、クライアント２、サーバ３間の暗号化通信に使用するものである。

【００４８】図５に示すように、前記相互認証が成立した後に、サーバ３は乱数Ｒｏをクライアント２に送信する。この乱数Ｒｏを受け取ったクライアント２は、ＩＣカード５に内部認証を要求する。これを受けて、ＩＣカード５は、Ｅ（Ｋａｉ［ｍ］，Ｒｏ）の処理を行なう。すなわち、不揮発性メモリ１２に記憶されている識別番号がｍ番の内部認証鍵を用いて乱数Ｒｏを暗号化し、このＥ（Ｋａｉ［ｍ］，Ｒｏ）をセッション鍵として用い、サーバ３と暗号化通信を行なう。同様に、サーバ３も、Ｅ（Ｋａｉ［ｍ］，Ｒｏ）の処理、すなわち、クライアント管理データベースに記憶されている識別番号がｍ番のクライアント２側の内部認証鍵を用いて乱数Ｒｏを暗号化し、このＥ（Ｋａｉ［ｍ］，Ｒｏ）をセッション鍵として、対称鍵暗号方式によりクライアント２と暗号化通信を行なう。

【００４９】つづいて、内部認証鍵、外部認証鍵の更新の手順について説明する。図６は、内部認証鍵、外部認証鍵を同時に更新するシーケンスの概念図である。一般にクライアント２／サーバ３間で相互認証、暗号化通信を行うには、前記のようにＩＣカード５に記憶されている認証鍵のうち、一番番号の大きいＫａｉ［ｍ］、Ｋａｅ［ｎ］を使用する。図６に示すように、暦で新しい月になってクライアント２から最初の接続要求がサーバ３にあったときに、図４を参照して前記した相互認証の処理に代えて、図６に示す処理を行う。

【００５０】すなわち、サーバ３は、乱数Ｒｓのみならず、認証鍵の更新要求と、相互認証しようする認証鍵の識別番号をクライアント２に送信する。数字の一番大きな識別番号は、内部認証鍵についてはｍ番、外部認証鍵についてはｎ番であるので、相互認証しようする認証鍵の識別番号として、ｍ番、ｎ番の上位認証鍵、すなわち、ｍ番、ｎ番より１番ずつ少ない、外部認証鍵については（ｍ－１）番、内部認証鍵については（ｎ－１）番をクライアント２に送信する。

【００５１】これを受け取ったクライアント２は、ＩＣカード５に内部認証要求を行ない、ＩＣカード５では、“内部認証コードＣａｉ＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｓ）”を求め、この内部認証コードＣａｉをクライアント２からサーバ３に送信する。そして、サーバ３では、“Ｒｓ’＝Ｄ（Ｋｓｅ［ｍ－１］，Ｃａｉ）”を求め、そして、ＲｓとＲｓ’とが一致するか否かを判断する。そして、一致するときはＯＫ信号を、一致しないときはＮＧ信号を、クライアント２に送信する。

【００５２】クライアント２がＯＫ信号を受けたときは、ＩＣカード５に乱数を要求する信号を出力する。ＩＣカード５は、この信号を受けて乱数Ｒａをクライアント２に出力し、クライアント２は乱数Ｒａをサーバ３に出力する。そして、サーバ３は、サーバ３の内部認証コード、すなわち、クライアント２にとっての外部認証コード“Ｃｓｉ＝Ｅ（Ｋｓｉ［ｎ－１］，Ｒａ）”を生成し、クライアント２に送信し、クライアント２は、この外部認証コードＣｓｉをＩＣカード５に送信する。そして、ＩＣカード５では、“Ｒａ’＝Ｄ（Ｋａｅ［ｎ－１］，Ｃｓｉ）”を求め、そしてＲａとＲａ’を比較して、一致するときはＯＫ信号を、一致しないときはＮＧ信号を、クライアント２に送り、上位認証鍵による相互認証が終了する。

【００５３】この相互認証終了後に認証鍵更新の処理に入る。すなわち、サーバ３は乱数Ｒｋ１、Ｒｋ２をクライアント２に送信する。また、サーバ３は、先程相互認証に用いたクライアント２側の内部認証鍵Ｋａｉ［ｍ－１］を用いて、“コードＣｓ１＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｋ１）”、“コードＣｓ２＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｋ２）”を求める。

【００５４】乱数Ｒｋ１、Ｒｋ２を受けたクライアント２は、まず、乱数Ｒｋ１を渡して、ＩＣカード５に内部認証を要求する。すると、ＩＣカード５は、“コードＣａ１＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｋ１）”を求め、このコードＣｓ１をクライアント２に送ると、クライアント２はコードＣａ１を新しい認証鍵とするようにＩＣカード５に要求する。そして、ＩＣカード５は、コードＣａ１をｍ番目の新しい内部認証鍵Ｋａｉ［ｍ］として不揮発性メモリ１２に記憶して、ＯＫ信号またはＮＧ信号を

クライアント２に送る。

【００５５】ＯＫ信号を受けたクライアント２は、次にＲｋ２を渡して、ＩＣカード５に内部認証を要求する。この要求を受けたＩＣカード５は、“コードＣａ２＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｋ２）”を求め、このコードＣａ２をクライアント２に送ると、クライアント２はコードＣａ２を新しい認証鍵とするようにＩＣカード５に要求する。そして、ＩＣカード５は、コードＣａ２をｎ番目の新しい内部認証鍵Ｋａｅ［ｎ］として不揮発性メモリ１２に記憶し、ＯＫ信号またはＮＧ信号をクライアント２に送る。クライアント２は受信したＯＫ信号をサーバ３に送信する。ＯＫ信号を受けたサーバ３は、すでに求めてあるコードＣｓ１を新しい外部認証鍵Ｋｓｅ［ｍ］としてクライアント管理データベースに記憶し、また、すでに求めてあるコードＣｓ２を新しい内部認証鍵Ｋｓｉ［ｎ］としてクライアント管理データベースに記憶して、認証鍵の更新を完了する。

【００５６】このようにして、最も番号の大きい内部認証鍵、外部認証鍵の更新がなされるが、この更新を１ヵ月に１度とはいえ、何度も繰り返していると、鍵の更新の際に使用している内部認証鍵Ｋａｉ［ｍ－１］、外部認証鍵Ｋａｅ［ｎ－１］も漏洩の可能性が高まる。そのような場合を考え、例えば１年に１度、内部認証鍵Ｋａｉ［ｍ－１］、外部認証鍵Ｋａｅ［ｎ－１］も更新する手続きをとるようにすればよい。その場合、更新の処理は図６を参照して説明した前記の処理と同様に行うことができる。すなわち、内部認証鍵Ｋａｉ［ｍ－２］、外部認証鍵Ｋａｅ［ｎ－２］を用いて、内部認証鍵Ｋａｉ［ｍ－１］、外部認証鍵Ｋａｅ［ｎ－１］を更新すればよい。以下、内部認証鍵Ｋａｉ［ｍ－２］、外部認証鍵Ｋａｅ［ｎ－２］、内部認証鍵Ｋａｉ［ｍ－３］、外部認証鍵Ｋａｅ［ｎ－３］、……についても同様である。

【００５７】すなわち、かかる認証鍵の更新は、更新の際の内部認証鍵の総数をＭ、外部認証鍵の総数をＮとしたときに、下式（１）で示されるｍ番目の内部認証鍵とｎ番目の外部認証鍵の更新を、識別番号が少なくともｍ番より小さい番号の内部認証鍵を用いてクライアント２がサーバ３を認証したことを条件に行なうもので、使用が稀である認証鍵により使用が頻繁な認証鍵ｍ番目の内部認証鍵とｎ番目の外部認証鍵とを安全に更新するものである。

【００５８】Ｍ－ｍ＝Ｎ－ｎ　……（１）

但し、上記の処理では、内部認証鍵Ｋａｉ［１］、外部認証鍵Ｋａｅ［１］は更新できないことになってしまう。内部認証鍵Ｋａｉ［１］、外部認証鍵Ｋａｅ［１］を更新する際には最初の相互認証そのものを内部認証鍵Ｋａｉ［１］、外部認証鍵Ｋａｅ［１］で行い、新しい鍵のもとになる乱数Ｒｋから新しい内部認証鍵Ｋａｉ［１］、外部認証鍵Ｋａｅ［１］を生成する際も内部認証鍵Ｋａｉ［１］を使用するという処理にしてもよい。

【００５９】しかし、実際の運用を考えた場合、内部認証鍵Ｋａｉ［１］、外部認証鍵Ｋａｅ［１］を更新する要求が発生するのは、内部認証鍵Ｋａｉ［１］、外部認証鍵Ｋａｅ［１］が漏洩した可能性がある場合である。その場合に、内部認証鍵Ｋａｉ［１］、外部認証鍵Ｋａｅ［１］を用いて鍵の更新を行うのは意味をなさない可能性があるので、内部認証鍵Ｋａｉ［１］、外部認証鍵Ｋａｅ［１］を更新する必要がある場合は、ＩＣカード５を鍵発行センタであるサーバ３に持参するか、ＩＣカード５を破棄して新しいＩＣカード５をサーバ３から受け取るのが望ましい。

【００６０】前記の例では、対称鍵暗号系を用いる場合について説明した。非対称鍵暗号系を用いる場合は次のようにする。

【００６１】すなわち、サーバ３は、各ユーザに対応して、ユーザ用に秘密鍵と公開鍵のペアをｍ組生成し、また、サーバ３用に秘密鍵と公開鍵のペアをｎ組生成する。そして、サーバ３のクライアント管理データベースには、サーバ３が生成したすべての秘密鍵、公開鍵を記憶する。

【００６２】基礎ファイルＩＥＦには、サーバ３でユーザ用にｍ組の秘密鍵と公開鍵のペアを生成して、そのうちの秘密鍵を内部認証鍵として記憶し、サーバ３用にｎ組の秘密鍵と公開鍵のペアを生成して、そのうちの公開鍵を外部認証鍵として記憶する。

【００６３】また、サーバ３のクライアント管理データベースは、サーバ３でユーザ用に生成した秘密鍵と公開鍵のペアのうちｍ組ある公開鍵を外部認証鍵として記憶し、サーバ３用に生成した秘密鍵と公開鍵のペアのうちｎ組ある秘密鍵を内部認証鍵として記憶する。

【００６４】以上の各点については、以下の各実施の形態で非対称鍵暗号系を用いる場合の説明においても同様である。

【００６５】以上のようにすることで、非対称鍵暗号系を用いる場合においても、その相互認証、セッション鍵の交換により行う暗号化データ通信、認証鍵の更新の処理は、図４～図６を参照して説明した対称鍵暗号系の場合と同様に行うことができる。なお、非対称鍵暗号系を用いて相互認証やセッション鍵交換を行う場合でも、暗号化データ通信を行う場合は対称鍵暗号方式を用いるのが一般的である。

【００６６】〔発明の第２の実施の形態〕この実施の形態は、相互認証、セッション鍵を交換して行う暗号化データ通信の手順は前記第１の実施の形態と同様であり、図示、説明は省略する。前記第１の実施の形態と同様の部材等については以下の説明で同一符号を付して説明する。

【００６７】この実施の形態では、認証鍵の更新のシーケンスが前記第１の実施の形態の場合と異なる。すなわち、前記第１の実施の形態では、外部認証鍵と内部認証

鍵とを一度に更新しているが、この実施の形態は個別的に更新を行うものである。

【００６８】図７は、この実施の形態の外部認証鍵の更新のシーケンスを示すブロック図である。但し、前記第１の実施の形態における図６に示すような上位認証鍵による相互認証の手続きは図示を省略しており、以下の説明でも省略する。すなわち、上位認証鍵による相互認証の手続きが完了すると、サーバ３からクライアント２に乱数Ｒｋ２を送信する。また、サーバ３は“コードＣｓ２＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｋ２）”を求める。クライアント２はＩＣカード５に乱数Ｒｋ２を送信し、内部認証を要求する。するとＩＣカード５は、“コードＣａ２＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｋ２）”を求め、このコードＣａ２をクライアント２に送信する。すると、クライアント２はコードＣａ２を新しい認証鍵とするようにＩＣカード５に要求する。そして、ＩＣカード５は、コードＣａ２をｎ番目の新しい内部認証鍵Ｋａｅ［ｎ］として不揮発性メモリ１２に記憶し、ＯＫ信号またはＮＧ信号をクライアント２に送る。クライアント２は受信したＯＫ信号をサーバ３に送信する。ＯＫ信号を受けたサーバ３は、すでに求めてあるコードＣｓ２を新しい外部認証鍵Ｋｓｉ［ｍ］としてクライアント管理データベースに記憶して、最も番号の大きい内部認証鍵Ｋａｉ［ｍ］の更新を完了する。

【００６９】図８は、この実施の形態の内部認証鍵の更新のシーケンスを示すブロック図である。但し、前記第１の実施の形態における図６に示すような上位認証鍵による相互認証の手続きは図示を省略しており、以下の説明でも省略する。すなわち、上位認証鍵による相互認証の手続きが完了すると、サーバ３からクライアント２に乱数Ｒｋ１を送信する。また、サーバ３は“コードＣｓ１＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｋ１）”を求める。クライアント２はＩＣカード５に乱数Ｒｋ１を送信し、内部認証を要求する。するとＩＣカード５は、“コードＣａ１＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｋ１）”を求め、このコードＣａ１をクライアント２に送信する。すると、クライアント２はコードＣａ１を新しい認証鍵とするようにＩＣカード５に要求する。そして、ＩＣカード５は、コードＣａ１をｎ番目の新しい内部認証鍵Ｋａｉ［ｎ］として不揮発性メモリ１２に記憶し、ＯＫ信号またはＮＧ信号をクライアント２に送る。クライアント２は受信したＯＫ信号をサーバ３に送信する。ＯＫ信号を受けたサーバ３は、すでに求めてあるコードＣｓ１を新しい内部認証鍵Ｋｓｅ［ｍ］としてクライアント管理データベースに記憶して、最も番号の大きい外部認証鍵Ｋａｅ［ｎ］の更新を完了する。

【００７０】〔発明の第３の実施の形態〕この実施の形態も、相互認証、セッション鍵を用いて行う暗号化データ通信の手順は前記第１の実施の形態と同様であり、図示、説明は省略する。前記第１の実施の形態と同様の部材等については以下の説明で同一符号を付して説明する。

【００７１】この実施の形態も、認証鍵の更新のシーケンスが前記第１の実施の形態の場合と異なる。すなわち、前記第１の実施の形態では、最も番号の大きい外部認証鍵と内部認証鍵のみを一度に更新しているが、この実施の形態は複数の外部認証鍵と内部認証鍵を一度に更新するものである。

【００７２】図９は、この実施の形態の外部認証鍵、内部認証鍵の更新のシーケンスを示すブロック図である。但し、前記第１の実施の形態における図６に示すような上位認証鍵による相互認証の手続きは図示を省略しており、以下の説明でも省略する。すなわち、上位認証鍵による相互認証の手続きが完了すると、前記第１の実施の形態と同様、認証鍵更新の処理に入る。

【００７３】すなわち、サーバ３は乱数Ｒｋ１、Ｒｋ２、Ｒｋ３、Ｒｋ４、……をクライアント２に送信する。また、サーバ３は、先程相互認証に用いた内部認証鍵Ｋａｉ［ｍ－１］を用いて、“コードＣｓ１＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｋ１）”、“コードＣｓ２＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｋ２）”、“コードＣｓ３＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｋ３）”、“コードＣｓ４＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｋ４）”、……を求める。

【００７４】乱数Ｒｋ１、Ｒｋ２、Ｒｋ３、Ｒｋ４、……を受けたクライアント２は、乱数Ｒｋ１、Ｒｋ２、Ｒｋ３、Ｒｋ４、……を送信し、ＩＣカード５に内部認証を要求する。すると、ＩＣカード５は、“コードＣａ１＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｋ１）”を求め、このコードＣａ１をクライアント２に送ると、クライアント２はコードＣａ１を新しい認証鍵とするようにＩＣカード５に要求する。そして、ＩＣカード５は、コードＣａ１をｍ番目の新しい内部認証鍵Ｋａｉ［ｍ］として不揮発性メモリ１２に記憶して、ＯＫ信号またはＮＧ信号をクライアント２に送る。

【００７５】ＯＫ信号を受けたクライアント２は、ＩＣカード５に内部認証を要求する。この要求を受けたＩＣカード５は、“コードＣａ２＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｋ２）”を求め、このコードＣａ２をクライアント２に送ると、クライアント２はコードＣａ２を新しい認証鍵とするようにＩＣカード５に要求する。そして、ＩＣカード５は、コードＣａ２をｎ番目の新しい外部認証鍵Ｋａｅ［ｎ］として不揮発性メモリ１２に記憶し、ＯＫ信号またはＮＧ信号をクライアント２に送る。

【００７６】ＯＫ信号を受けたクライアント２は、ＩＣカード５に内部認証を要求する。すると、ＩＣカード５は、“コードＣａ３＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｋ３）”を求め、このコードＣａ３をクライアント２に送ると、クライアント２はコードＣａ３を新しい認証鍵とするようにＩＣカード５に要求する。そして、ＩＣカード５は、コードＣａ３をｍ＋１番目の新しい内部認証鍵

Ｋａｉ［ｍ＋１］として不揮発性メモリ１２に記憶して、ＯＫ信号またはＮＧ信号をクライアント２に送る。

【００７７】ＯＫ信号を受けたクライアント２は、ＩＣカード５に内部認証を要求する。この要求を受けたＩＣカード５は、“コードＣａ４＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｋ４）”を求め、このコードＣａ４をクライアント２に送ると、クライアント２はコードＣａ４を新しい認証鍵とするようにＩＣカード５に要求する。そして、ＩＣカード５は、コードＣａ４をｎ番目の新しい外部認証鍵Ｋａｅ［ｎ＋１］として不揮発性メモリ１２に記憶し、ＯＫ信号またはＮＧ信号をクライアント２に送る。

【００７８】以上のような処理を繰り返した後、クライアント２は受信したＯＫ信号をサーバ３に送信する。ＯＫ信号を受けたサーバ３は、すでに求めてあるコードＣａ１を新しい外部認証鍵Ｋｓｅ［ｍ］とし、また、コードＣａ２を新しい内部認証鍵Ｋｓｉ［ｎ］とし、コードＣｓ３を新しい外部認証鍵Ｋｓｅ［ｍ＋１］とし、また、コードＣｓ４を新しい内部認証鍵Ｋｓｉ［ｎ＋１］、……として、クライアント管理データベースに記憶し、認証鍵の更新を完了する。

【００７９】〔発明の第４の実施の形態〕この実施の形態も、相互認証、セッション鍵を用いて行う暗号化データ通信の手順は前記第１の実施の形態と同様であり、図示、説明は省略する。前記第１の実施の形態と同様の部材等については以下の説明で同一符号を付して説明する。

【００８０】この実施の形態も、認証鍵の更新のシーケンスが前記第１の実施の形態の場合と異なる。すなわち、前記第１の実施の形態では、ＩＣカード５で新たな認証鍵を計算し、その結果をクライアント２に送信しているが、この実施の形態では、クライアント２に送信せずに、新たな認証鍵の計算し、それをＩＣカード５内に設定するものである。

【００８１】図１０は、この実施の形態の外部認証鍵、内部認証鍵の更新のシーケンスを示すブロック図である。但し、前記第１の実施の形態における図６に示すような上位認証鍵による相互認証の手続きは図示を省略しており、以下の説明でも省略する。すなわち、上位認証鍵による相互認証の手続きが完了すると、前記第１の実施の形態と同様、認証鍵更新の処理に入る。

【００８２】すなわち、サーバ３は乱数Ｒｋ１、Ｒｋ２をクライアント２に送信する。また、サーバ３は、先程相互認証に用いた内部認証鍵Ｋａｉ［ｍ－１］を用いて、“コードＣｓ１＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｋ１）”、“コードＣｓ２＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｋ２）”を求める。

【００８３】乱数Ｒｋ１、Ｒｋ２を受けたクライアント２は、乱数Ｒｋ１，Ｒｋ２を送信し、ＩＣカード５に内部認証を要求する。すると、ＩＣカード５は、“コードＣａ１＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｋ１）”を求め、このコードＣａ１をクライアント２に送ることなく、コードＣａ１をｍ番目の新しい内部認証鍵Ｋａｉ［ｍ］として不揮発性メモリ１２に記憶して、ＯＫ信号またはＮＧ信号をクライアント２に送る。

【００８４】ＯＫ信号を受けたクライアント２はＩＣカード５に内部認証を要求する。この要求を受けたＩＣカード５は、“コードＣａ２＝Ｅ（Ｋａｉ［ｍ－１］，Ｒｋ２）”を求め、このコードＣａ２をクライアント２に送ることなく、コードＣａ２をｎ番目の新しい内部認証鍵Ｋａｅ［ｎ］として不揮発性メモリ１２に記憶し、ＯＫ信号またはＮＧ信号をクライアント２に送る。クライアント２は受信したＯＫ信号をサーバ３に送信する。ＯＫ信号を受けたサーバ３は、すでに求めてあるコードＣａ１を新しい外部認証鍵Ｋｓｅ［ｍ］としてクライアント管理データベースに記憶し、また、すでに求めてあるコードＣｓ２を新しい内部認証鍵Ｋｓｉ［ｎ］としてクライアント管理データベースに記憶して、１番大きな番号の認証鍵の更新を完了する。

【００８５】内部認証鍵Ｋａｉ［ｍ－１］、外部認証鍵Ｋａｅ［ｎ－１］、内部認証鍵Ｋａｉ［ｍ－２］、外部認証鍵Ｋａｅ［ｎ－２］、……の更新についても、前記と同様に更新することができる。

【００８６】なお、いうまでもなく、前記各実施の形態は、この発明を限定するものではない。

【００８７】例えば、前記各実施例で、サーバ３では、“Ｄ（Ｋｓｅ〔ｍ〕、Ｅ（Ｋａｉ〔ｍ〕，Ｒｓ））”の処理を行い、そして、この復号化した“Ｄ（Ｋｓｅ〔ｍ〕，Ｅ（Ｋａｉ〔ｍ〕，Ｒｓ））”と乱数Ｒｓとが一致するか否かを判断しているが、対称鍵暗号系を用いる場合は、これに代えて、Ｅ（Ｋｓｅ〔ｍ〕，Ｒｓ）とＥ（Ｋａｉ〔ｍ〕，Ｒｓ）とが一致するか否かを判断するようにしてもよいし、前記の例では、ＩＣカード５で“Ｄ（Ｋａｅ〔ｎ〕，Ｅ（Ｋｓｉ〔ｎ〕，Ｒａ））”の処理を行い、そして、この復号化した“Ｄ（Ｋａｅ〔ｎ〕，Ｅ（Ｋｓｉ〔ｎ〕，Ｒａ））”と乱数Ｒａとが一致するか否かを判断しているが、これに代えて、Ｅ（Ｋａｅ〔ｎ〕，Ｒａ）とＥ（Ｋｓｉ〔ｎ〕，Ｒａ）とが一致するか否かを判断するようにしてもよい。

【００８８】また、前記第１、第２、第４の実施の形態で、乱数Ｒｋ１、Ｒｋ２の両方を送信しなくても、乱数Ｒｋ１のみを送信し、このＲｋ１の補数を乱数Ｒｋ２の代わりに用いるというように、Ｒｋ１からＲｋ２を導き出すようにしてもよい。

【００８９】

【発明の効果】請求項１に記載の発明は、通信回線を介して接続されているクライアントとサーバとの間の相互認証に使用する認証鍵を格納している記憶媒体をユーザが所持し、この記憶媒体と前記クライアントを接続して、前記認証鍵を用いた前記相互認証を行なった後、前記認証鍵に基づいてセッション鍵を生成して暗号化通信

を行なうネットワークシステムであって、前記認証鍵は前記記憶媒体に複数個記憶して、定期または不定期に更新して用い、この更新を前記複数の認証鍵のうちいずれかのものに対して行なうには、少なくとも当該認証鍵以外の前記認証鍵を用いて行なう前記相互認証が成立した後に、前記サーバから乱数を前記クライアントに送信し、前記相互認証に用いた前記認証鍵を用いて前記乱数から更新にかかる前記認証鍵を新たに生成して前記記憶媒体に記憶することにより行なうものであることを特徴とするものであるため、相互認証が成立した後に、サーバから乱数をクライアントに送信し、相互認証に用いた認証鍵を用いて乱数から更新にかかる認証鍵を新たに暗号化や復号化などで生成することができるので、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、認証鍵を更新することができる。

【００９０】請求項２に記載の発明は、請求項１に記載の発明において、記憶媒体は、クライアントがサーバを認証するための認証鍵である外部認証鍵と、前記サーバが前記クライアントを認証するための認証鍵である内部認証鍵とをいずれも識別番号を付して複数個ずつ記憶していて、前記内部認証鍵および前記外部認証鍵を用いて相互認証を行なうものであることを特徴とするものであるため、相互認証が成立した後に、サーバから乱数をクライアントに送信し、相互認証に用いた内部認証鍵を用いて乱数から更新にかかる内部認証鍵、外部認証鍵を新たに生成することができるので、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、内部認証鍵、外部認証鍵を更新することができる。

【００９１】請求項３に記載の発明は、請求項２に記載の発明において、複数の内部認証鍵のうち識別番号がｍ番のものを更新するには、外部認証鍵と少なくともこのｍ番の内部認証鍵以外の内部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記ｍ番の内部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものであるため、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、識別番号がｍ番の内部認証鍵を更新することができる。

【００９２】請求項４に記載の発明は、請求項２または３のいずれかに記載の発明において、複数の外部認証鍵のうち識別番号がｎ番のものを更新するには、内部認証鍵と少なくともこのｎ番の外部認証鍵以外の外部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記ｎ番の外部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものであるため、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに識別番号がｎ番の外部認証鍵を更新することができる。

【００９３】請求項５に記載の発明は、請求項２、３、４のいずれかに記載の発明において、複数の内部認証鍵のうち識別番号がｍ番のものおよび複数の外部認証鍵のうち識別番号がｎ番目のものを一度に更新するには、少なくとも前記ｍ番の内部認証鍵以外の内部認証鍵と少なくとも前記ｎ番の外部認証鍵以外の外部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記ｍ番の内部認証鍵と前記ｎ番の外部認証鍵とを新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものであるため、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、少ない鍵更新処理により安全に、識別番号がｍ番の内部認証鍵と識別番号がｎ番の外部認証鍵を一度に更新することができる。

【００９４】請求項６に記載の発明は、請求項２、３、４、５のいずれかに記載の発明において、複数の内部認証鍵を一度に更新するには、外部認証鍵と識別番号がｍ番より小さい内部認証鍵とを用いて相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記識別番号がｍ番以上の各内部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものであるため、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、少ない鍵更新処理により安全に、複数の内部認証鍵を一度に更新することができる。

【００９５】請求項７に記載の発明は、請求項２、３、４、５、６のいずれかに記載の発明において、複数の外部認証鍵を一度に更新するには、内部認証鍵と識別番号がｎ番より小さい外部認証鍵とを用いて相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記識別番号がｎ番以上の各外部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものであるため、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、少ない鍵更新処理により安全に、複数の外部認証鍵を一度に更新することができる。

【００９６】請求項８に記載の発明は、請求項２、３、４、５、６、７のいずれかに記載の発明において、複数の内部認証鍵と複数の外部認証鍵とを一度に更新するには、識別番号がｍ番より小さい内部認証鍵と識別番号がｎ番より小さい外部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から識別番号がｍ番以上の内部認証

鍵と識別番号がｎ番移動の外部認証鍵とを新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものであるため、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、少ない鍵更新処理により安全に、複数の内部認証鍵と複数の外部認証鍵とを一度に更新することができる。

【００９７】請求項９に記載の発明は、請求項２、３、４、５、６、７、８のいずれかに記載の発明において、更新の際の内部認証鍵の総数をＭ、外部認証鍵の総数をＮとしたときに、下式で示されるｍ番目の内部認証鍵とｎ番目の外部認証鍵の更新は、識別番号が少なくともｎ番より小さい番号の外部認証鍵を用いてクライアントがサーバを認証したことを条件に行なうものであることを特徴とするものであるため、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、使用が稀である認証鍵により使用が頻繁な認証鍵ｍ番目の内部認証鍵とｎ番目の外部認証鍵とを安全に更新することができる。

【００９８】Ｍ－ｍ＝Ｎ－ｎ

請求項１０に記載の発明は、請求項２、３、４、５、６、７、８、９のいずれかに記載の発明において、記憶媒体は、更新に先立って行なわれた相互認証に使用した認証鍵を用いサーバがクライアントに送信した乱数から新たな認証鍵の生成を行なって、この生成後の新たな認証鍵を記憶媒体内部の不揮発性メモリにのみ記憶するものであることを特徴とするものであるため、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、更新後の新たな認証鍵を記憶媒体外に漏らすことなく認証鍵を安全に更新することができる。

【００９９】請求項１１に記載の発明は、請求項２、３、４、５、６、７、８、９、１０のいずれかに記載の発明において、記憶媒体としてＩＣカードを用いることを特徴とするものであるため、一般に普及し始めているＩＣカードを記憶媒体としてもちい、ネットワークシステムを低コストで構築することができる。

【図面の簡単な説明】

【図１】この発明の第１の実施の形態にかかるネットワークシステムの概略構成を示すブロック図である。

【図２】前記ネットワークシステムに用いるＩＣカードの回路構成を示すブロック図である。

【図３】前記ＩＣカード内の不揮発メモリ内の認証鍵のファイルフォーマットの一例を示すブロック図である。

【図４】前記ネットワークシステムにおける相互認証の処理手順を示すブロック図である。

【図５】前記ネットワークシステムにおける暗号化データ通信に用いるセッション鍵の生成の手順を示すブロック図である。

【図６】前記ネットワークシステムにおける内部認証鍵、外部認証鍵の更新の手順を示すブロック図である。

【図７】この発明の第２の実施の形態にかかるネットワークシステムにおける外部認証鍵の更新手順を示すブロック図である。

【図８】この発明の第２の実施の形態にかかるネットワークシステムにおける内部認証鍵の更新手順を示すブロック図である。

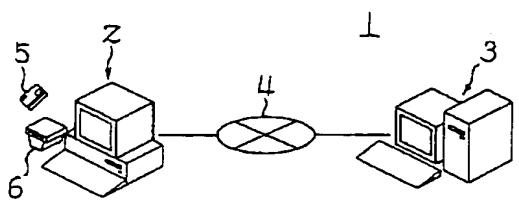
【図９】この発明の第３の実施の形態にかかるネットワークシステムにおける内部認証鍵、外部認証鍵の更新手順を示すブロック図である。

【図１０】この発明の第４の実施の形態にかかるネットワークシステムにおける内部認証鍵、外部認証鍵の更新手順を示すブロック図である。

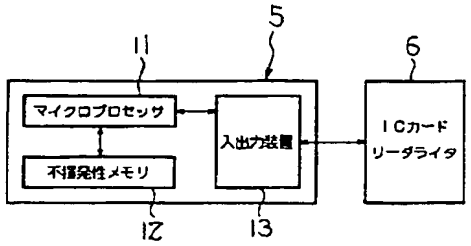
【符号の説明】

１　　ネットワークシステム
２　　クライアント
３　　サーバ
４　　通信回線
５　　記憶媒体（ＩＣカード）
１２　　不揮発性メモリ

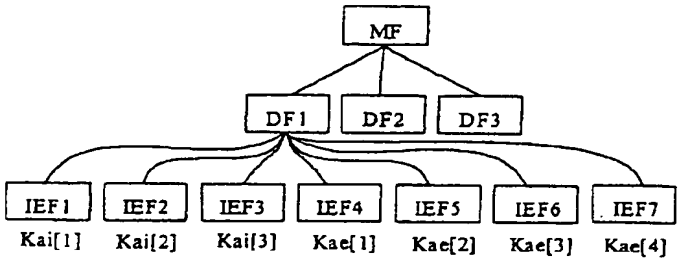
【図１】



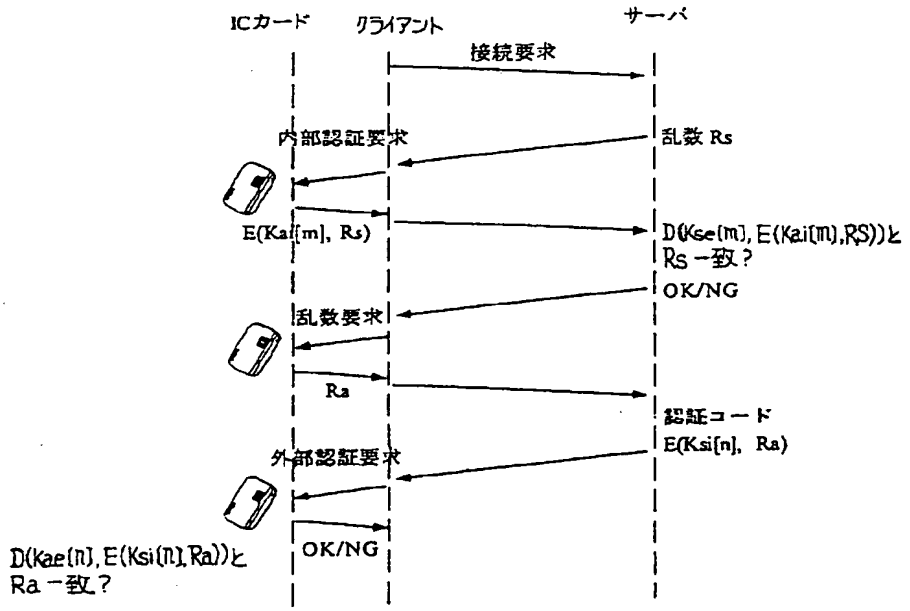
【図２】



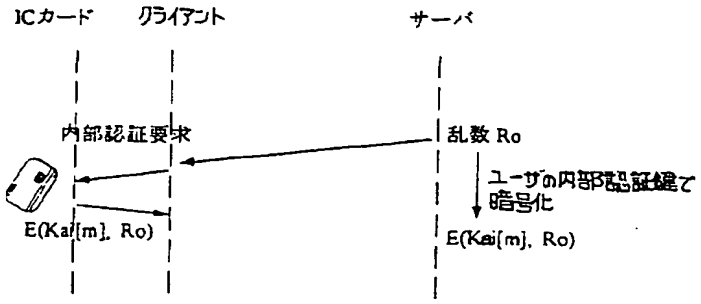
【図３】


MF
DF1
DF2
DF3
IEF1
IEF2
IEF3
IEF4
IEF5
IEF6
IEF7
Kai[1]
Kai[2]
Kai[3]
Kae[1]
Kae[2]
Kae[3]
Kae[4]

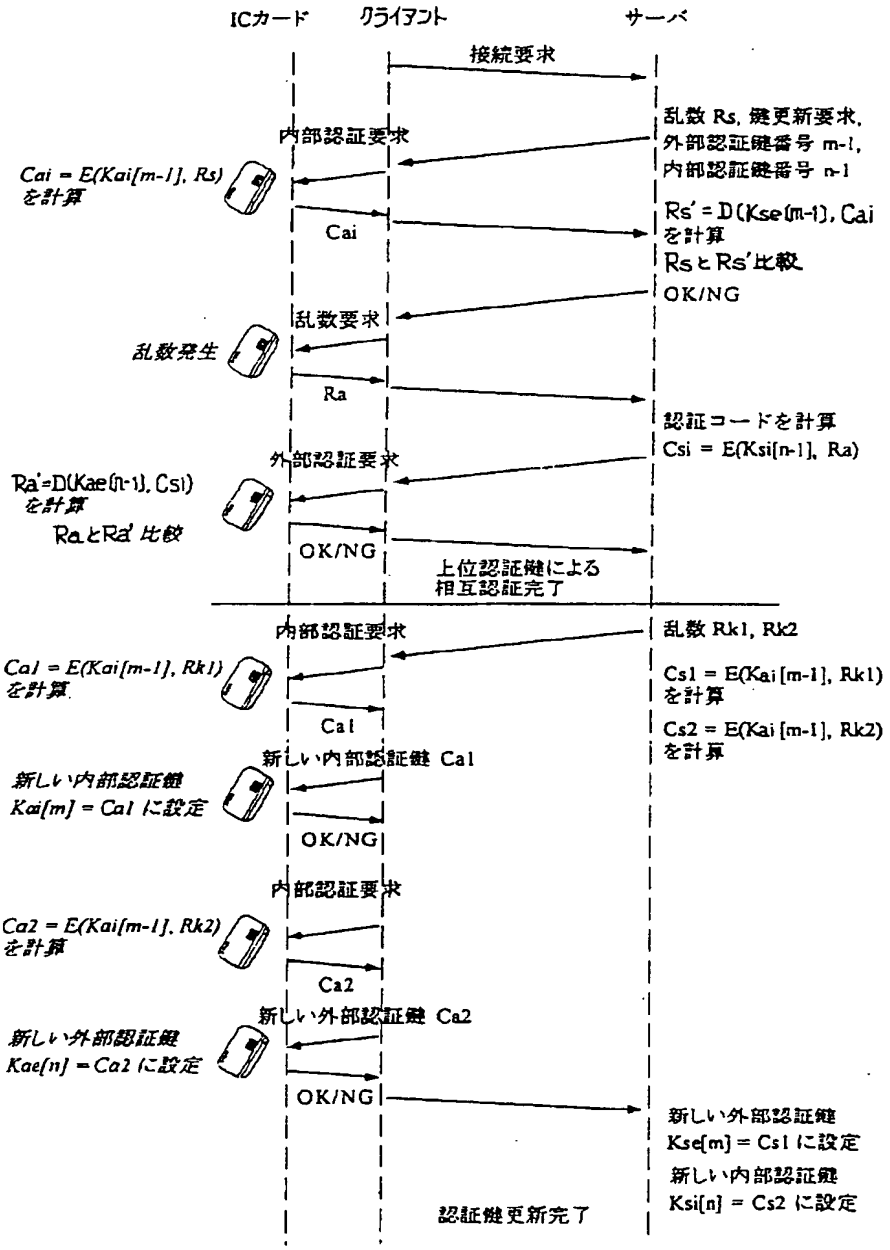
【図４】


ICカード
クライアント
サーバ
接続要求
内部認証要求
乱数 Rs
E(Kai[m], Rs)
D(Kse[m], E(Kai[m],RS))と
Rs一致？
OK/NG
乱数要求
Ra
認証コード
E(Ksi[n], Ra)
外部認証要求
OK/NG
D(Kae[n], E(Ksi[n],Ra))と
Ra一致？

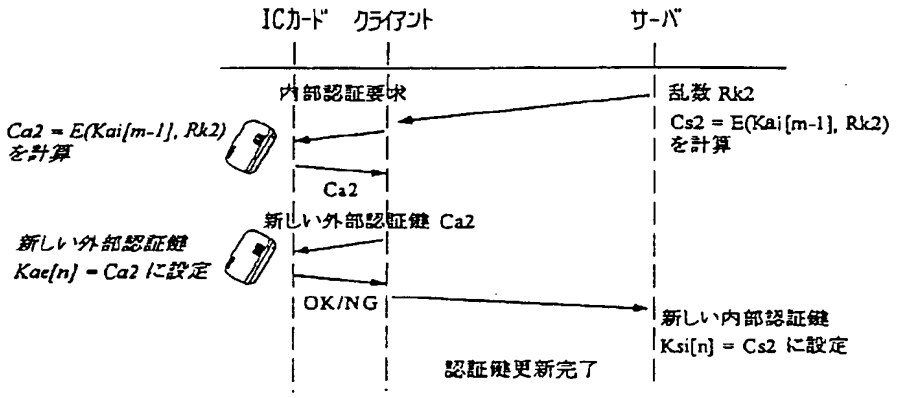
【図５】


ICカード
クライアント
サーバ
内部認証要求
乱数 Ro
ユーザの内部認証鍵で
暗号化
E(Kai[m], Ro)
E(Kai[m], Ro)

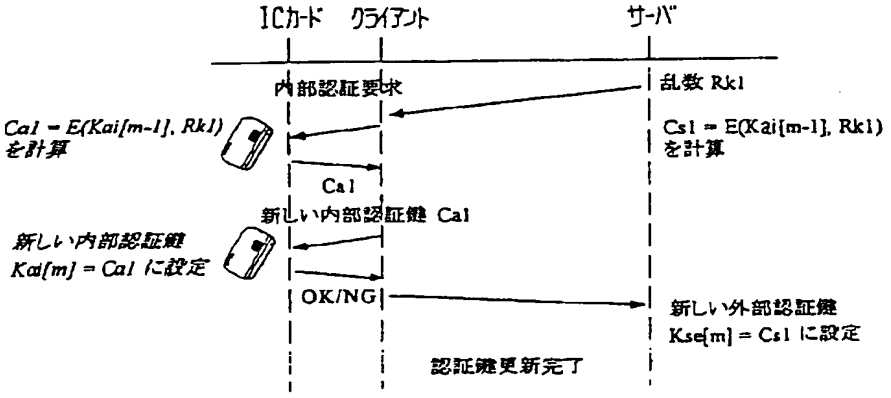
【図６】


ICカード
クライアント
サーバ
接続要求
乱数 Rs, 鍵更新要求,
外部認証鍵番号 m-1,
内部認証鍵番号 n-1
内部認証要求
Cai = E(Kai[m-1], Rs)
を計算
Cai
Rs' = D(Kse[m-1], Cai
を計算
Rs と Rs' 比較
OK/NG
乱数要求
乱数発生
Ra
認証コードを計算
Csi = E(Ksi[n-1], Ra)
外部認証要求
Ra'=D(Kae[n-1], Csi)
を計算
Ra と Ra' 比較
OK/NG
上位認証鍵による
相互認証完了
内部認証要求
乱数 Rk1, Rk2
Ca1 = E(Kai[m-1], Rk1)
を計算
Cs1 = E(Kai[m-1], Rk1)
を計算
Ca1
Cs2 = E(Kai[m-1], Rk2)
を計算
新しい内部認証鍵 Ca1
新しい内部認証鍵
Kai[m] = Ca1 に設定
OK/NG
内部認証要求
Ca2 = E(Kai[m-1], Rk2)
を計算
Ca2
新しい外部認証鍵 Ca2
新しい外部認証鍵
Kae[n] = Ca2 に設定
OK/NG
新しい外部認証鍵
Kse[m] = Cs1 に設定
新しい内部認証鍵
Ksi[n] = Cs2 に設定
認証鍵更新完了

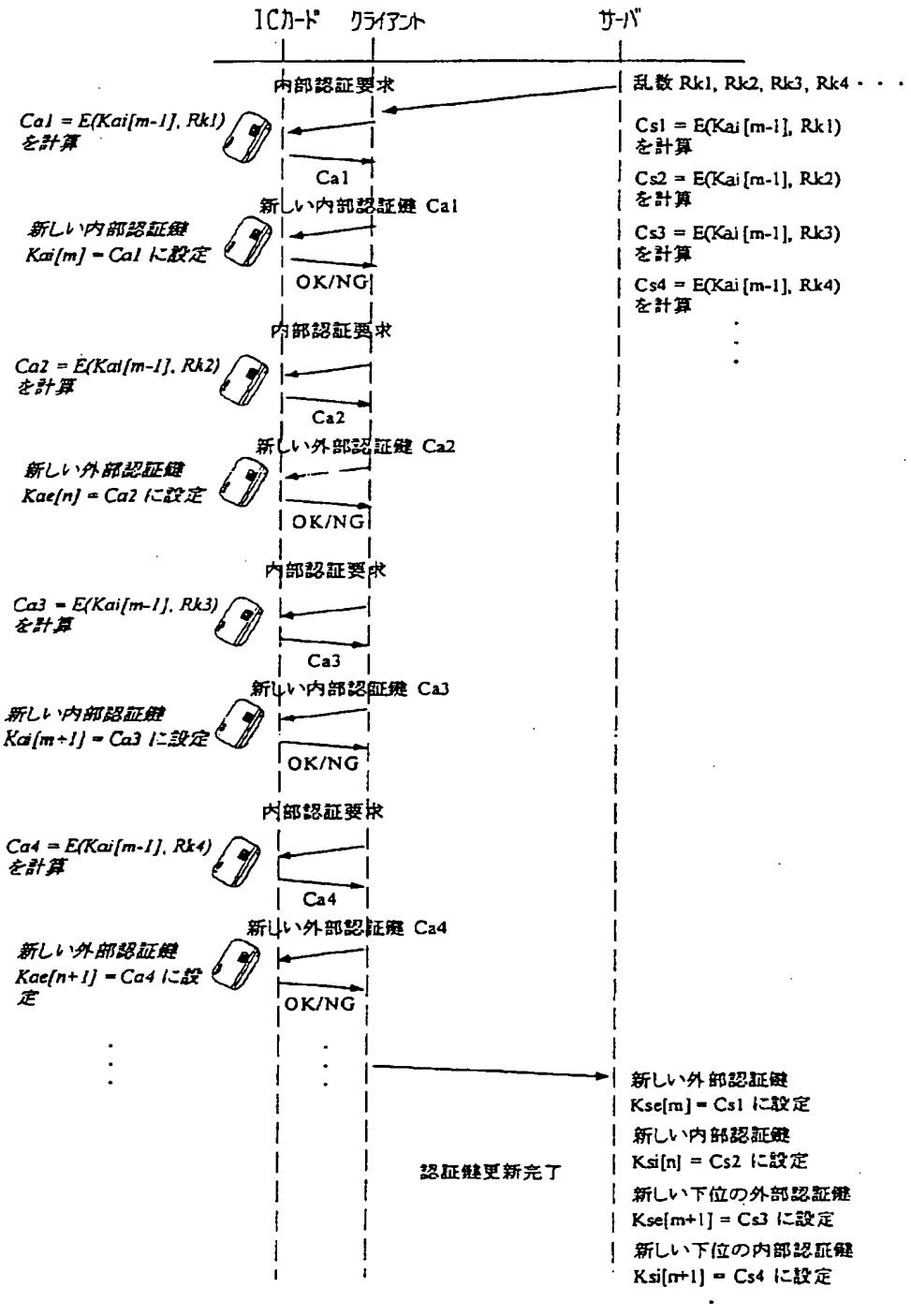
【図７】


ICカード
クライアント
サーバ
内部認証要求
乱数 Rk2
Cs2 = E(Kai[m-1], Rk2)
を計算
Ca2 = E(Kai[m-1], Rk2)
を計算
Ca2
新しい外部認証鍵 Ca2
新しい外部認証鍵
Kae[n] = Ca2 に設定
OK/NG
新しい内部認証鍵
Ksi[n] = Cs2 に設定
認証鍵更新完了

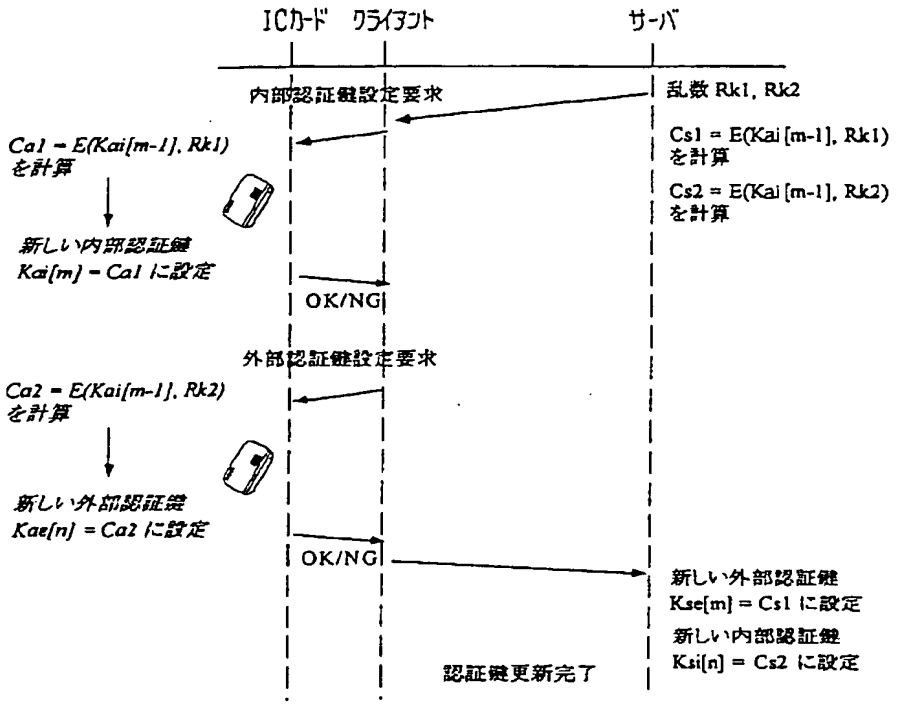
【図８】


ICカード
クライアント
サーバ
内部認証要求
乱数 Rk1
Cs1 = E(Kai[m-1], Rk1)
を計算
Ca1 = E(Kai[m-1], Rk1)
を計算
Ca1
新しい内部認証鍵 Ca1
新しい内部認証鍵
Kai[m] = Ca1 に設定
OK/NG
新しい外部認証鍵
Kse[m] = Cs1 に設定
認証鍵更新完了

【図９】


ICカード
クライアント
サーバ
内部認証要求
乱数 Rk1, Rk2, Rk3, Rk4・・・
Ca1 = E(Kai[m-1], Rk1) を計算
Cs1 = E(Kai[m-1], Rk1) を計算
Ca1
Cs2 = E(Kai[m-1], Rk2) を計算
新しい内部認証鍵 Ca1
新しい内部認証鍵 Kai[m] = Ca1 に設定
Cs3 = E(Kai[m-1], Rk3) を計算
OK/NG
Cs4 = E(Kai[m-1], Rk4) を計算
内部認証要求
Ca2 = E(Kai[m-1], Rk2) を計算
Ca2
新しい外部認証鍵 Ca2
新しい外部認証鍵 Kae[n] = Ca2 に設定
OK/NG
内部認証要求
Ca3 = E(Kai[m-1], Rk3) を計算
Ca3
新しい内部認証鍵 Ca3
新しい内部認証鍵 Kai[m+1] = Ca3 に設定
OK/NG
内部認証要求
Ca4 = E(Kai[m-1], Rk4) を計算
Ca4
新しい外部認証鍵 Ca4
新しい外部認証鍵 Kae[n+1] = Ca4 に設定
OK/NG
新しい外部認証鍵 Kse[m] = Cs1 に設定
新しい内部認証鍵 Ksi[n] = Cs2 に設定
認証鍵更新完了
新しい下位の外部認証鍵 Kse[m+1] = Cs3 に設定
新しい下位の内部認証鍵 Ksi[n+1] = Cs4 に設定

【図１０】



フロントページの続き

(51) Int. Cl.⁶	識別記号	FI
		H04L 9/00　675A